

SSLCERT API Reference

API Reference for managing SSL Certificates

Version 1.0
September 16, 2005

Proprietary Information

This document is our property. It may be used by recipient only for the purpose for which it was transmitted and shall be returned upon request or when no longer needed by recipient. It may not be copied or communicated without the prior written consent of us.

COPYRIGHT NOTIFICATION

Copyright © 2005. All rights reserved.

DISCLAIMER AND LIMITATION OF LIABILITY

We made efforts to ensure the accuracy and completeness of all information in this document. However, we make no warranties of any kind (whether express, implied or statutory) with respect to the information herein. We assume no liability to any party for loss or damage (whether direct or indirect) caused by any errors, omissions or statements of any kind contained in this document. Further, we assume no liability arising from the application or use of the product or service described herein and specifically disclaims any representation that the products or services described herein do not infringe upon any existing or future intellectual property rights. Nothing herein grants the reader any license to make, use, or sell equipment or products constructed in accordance with this document. Finally, all rights and privileges related to any intellectual property right described herein are vested in the patent, trademark, or service mark owner, and no other person may exercise such rights without express permission, authority, or license secured from the patent, trademark, or service mark owner.

We reserve the right to make changes to any information herein without further notice.

NOTICE AND CAUTION concerning Patent or Trademark Rights

The inclusion in this document, the associated on-line file, or the associated software of any information covered by any patent, trademark, or service mark rights shall not constitute nor imply a grant of, or authority to exercise, any right or privilege protected by such patent, trademark, or service mark. All such rights and privileges are vested in the patent, trademark, or service mark owner, and no other person may exercise such rights without express permission, authority, or license secured from the patent, trademark, or service mark owner.

This publication was created using OpenOffice.org by Sun Microsystems Inc.

SSLCERT API Reference
Version 1.0

TABLE OF CONTENTS

1. Introduction.....	4
2. SSLCERT User Relations.....	5
3. SSLCERT Environment DB.....	6
4. Commands.....	7
4.1 SSLCERT Commands.....	8
4.1.1 CreateSSLCert.....	9
4.1.2 StatusSSLCert.....	11
4.1.3 QuerySSLCertList.....	12
4.1.4 ParseSSLCertCSR.....	14

1. Introduction

This manual describes the API commands for the ordering of SSL Certificates through the system.

SSL (Secure Socket Layer) is the standard protocol for transaction security used worldwide. SSL-Connection basically submits all information between your servers and the customers browser in an encrypted form, meaning that all information is kept absolutely confidential.

Our API is connected to Thawte, a VeriSign Inc. Company, and Comodo Inc., two of the major SSL certificate suppliers worldwide.

The following products are offered through our API:

- Comodo InstantSSL
- Comodo IntranetSSL
- Comodo WildcardSSL
- Thawte SSL123

The API itself is not object orientated, but object related and can be encapsulated into any OO language without much hassle.

If there are any errors or missing topics, please don't hesitate to contact us.

2. SSLCERT User Relations

The relations define the operational parameters of a user and can only be modified by its superordinate users. The most important use of relations is to define the prices.

The system currently supports the following relation types for SSLCERTs:

Relation type	Description
SSLCERT_COMODO_INSTANTSSL_ANNUAL	Annual fee for a Comodo InstantSSL Certificate
SSLCERT_COMODO_INSTANTSSL_SETUP	Additional setup fee for the Comodo InstantSSL Certificate
SSLCERT_COMODO_INTRANETSSL_ANNUAL	Annual fee for a Comodo IntranetSSL Certificate
SSLCERT_COMODO_INTRANETSSL_SETUP	Additional setup fee for the Comodo IntranetSSL Certificate
SSLCERT_COMODO_WILDCARDSSL_ANNUAL	Annual fee for a Comodo WildcardSSL Certificate
SSLCERT_COMODO_WILDCARDSSL_SETUP	Additional setup fee for the Comodo WildcardSSL Certificate
SSLCERT_THAWTE_SSL123_ANNUAL1	Annual fee for a Thawte SSL123 Certificate
SSLCERT_THAWTE_SSL123_SETUP	Additional setup fee for the Thawte SSL123 Certificate
SSLCERT_COMODO_INSTANTSSL_CURRENCY	Currency that is used (ANNUAL/SETUP) for Comodo InstantSSL
SSLCERT_COMODO_INTRANETSSL_CURRENCY	Currency that is used (ANNUAL/SETUP) for Comodo IntranetSSL
SSLCERT_COMODO_WILDCARDSSL_CURRENCY	Currency that is used (ANNUAL/SETUP) for Comodo WildcardSSL
SSLCERT_THAWTE_SSL123_CURRENCY	Currency that is used (ANNUAL/SETUP) for Thawte SSL123

Prices are calculated according to the daily exchange rate of the ECB (European Central Bank, www.ecb.int), if the SSLCERT relation currency and user account currency are different!

3. SSLCERT Environment DB

There are currently no environment keys used for SSLCERTs.

4. Commands

All SSLCERT related commands can be submitted through the default API Gateways as described in the core API reference manual.

4.1 SSLCERT Commands

4.1.1 CreateSSLCert

Description

The command creates a new SSL Cert order, using a CSR (Certificate Sign Request) and some other personal data (i.e. Contact-Address) that must be provided by you within the request struct.

Availability

No limitations.

Input Parameters

submit the request using the following syntax:

```
BASE-URL?s_login=reseller.de&s_pw=secret&command=command&parameter1=value1&parameter2=value2&parameter3=value3...
```

Parameter	Obligation	Definition	Type
s_login	required	Login ID of the user account	TEXT
s_pw	required	Account password	TEXT
s_user	optional	User ID of the user as which the command shall be executed (must be a subuser of s_login)	TEXT
command	required	Name of command to be executed, here: command = CreateSSLCert	TEXT
sslcertclass	required	Choose the type of product, possible values: COMODO_INSTANTSSL COMODO_INTRANETSSL COMODO_WILDCARDSSL THAWTE_SSL123	TEXT
period	optional	Expiretime of the signed certificate in years (default = 1 year)	INTEGER
name	Required only for Comodo	Your full name in the form "\$firstname \$lastname". This parameter is mandatory for Comodo and ignored by Thawte.	TEXT
firstname	Required only for Thawte	Your firstname. This parameter is mandatory for Thawte and is ignored by Comodo	TEXT
lastname	Required only for Thawte	Your lastname. This parameter is mandatory for Thawte and is ignored by Comodo	TEXT
street	required	Your Address	TEXT
zip	required	Your postal code	TEXT
city	required	Your city	TEXT
province	optional	State or province	TEXT
csr0...csrN	required	The certificate sign request (CSR) by line, represented as csr0, csr1, csr2, ... , csrN: csr0 = -----BEGIN CERTIFICATE REQUEST----- csr1 = A34)\$/45BF... csr2 = GG.. csr3 = ... csrN = -----END CERTIFICATE REQUEST-----	TEXT
jobtitle	Required only for Thawte	Your job title or position within your company. That parameter is ignored by Comodo.	TEXT
phone	Required only for Thawte	Your phone number. That parameter is ignored by Comodo.	TEXT

Parameter	Obligation	Definition	Type
Email	Required only for Thawte	Your email address. This parameter is ignored by Comodo.	TEXT

Returned Properties and Values

Code	Description
200	Command completed successfully
504	The command failed due to a missing or misspelled parameter
541	The command failed due to an internal error, i.e. if a nonexisting sslcertclass has been chosen

Property	Description
sslcertid	The unique object ID number (16 hex digits) in our system
sslcertclass	The sslcertclass as chosen in the request
status	After the placed order the initial status is always "PENDING"
createddate	Date/Time of the order
updateddate	Not of interest yet for ssl certificates
expirationdate	Date/Time of the expiration

Notes:

- Comodo certificates are normally issued within 1 minute, Thawte certificate are issued within some minutes.

4.1.2 StatusSSLCert

Description

Query your certificate sign request, the availability status of a cert, the signed cert data and expiration informations.

Availability

The SSLcert-ID must exist.

Input Parameters

submit the request using the following syntax:

```
BASE-URL?s_login=reseller.de&s_pw=secret&command=command&parameter1=value1&parameter2=value2&parameter3=value3...
```

Parameter	Obligation	Definition	Type
s_login	required	Login ID of the user account	TEXT
s_pw	required	Account password	TEXT
s_user	optional	User ID of the user as which the command shall be executed (must be a subuser of s_login)	TEXT
command	required	Name of command to be executed, here: command=StatusSSLCert	TEXT
sslcertid	required	The unique ID of the SSL-Cert ordering process	TEXT

Returned Properties and Values

Code	Description
200	Command completed successfully
541	The command failed because the chosen sslcertid is not assigned
504	Missing Parameter

Property	Description
sslcertid	The unique object ID number (16 hex digits) in our system
sslcertclass	The sslcertclass as chosen in the request
status	PENDING, if certificate has not been issued yet ACTIVE, if certificate has been issued.
createddate	Date/Time of the order
updateddate	Not of interest yet for ssl certificates
expirationdate	Date/Time of the expiration
csr0...csrN	Your certificate sign request by line (csr0, csr1, ... , csrN)
crt0...crtN	Your signed certificate by line (crt0, crt1, ... , crtN)

Notes:

- The CRT property of Thawte's certificates contains only the signed cert itself, because nothing other is needed for the installation in an apache webserver. The CRT property of Comodo's certificates contains (in that order) the signed cert, the intermediate cert, the root certificate.

4.1.3 QuerySSLCertList

Description

The command queries a list of all your cert orders.

Availability

Always.

Input Parameters

submit the request using the following syntax:

```
BASE-URL?s_login=reseller.de&s_pw=secret&command=command&parameter1=value1&parameter2=value2&parameter3=value3...
```

Parameter	Obligation	Definition	Type
s_login	required	Login ID of the user account	TEXT
s_pw	required	Account password	TEXT
command	required	Name of command to be executed, here: QuerySSLCertList	TEXT
userdepth	optional	Possible values: SELF (only own objects) SUBUSER (only your subusers' objects) ALL (your own and your subusers' objects)	TEXT
wide	optional	Possible values: 0 or 1 If set to "1" advanced response information is given back	INTEGER
first	optional	Shows only objects beginning from objectindex "first", default: first=0	INTEGER
last	optional	Shows only the objects to the objectindex "last", default: inf	INTEGER
limit	optional	Shows only that amount of objects, default: limit=1000. First, Last & Limit are similar used as in a SQL query string (i.e. "SELECT x,y,z FROM tab LIMIT first,limit")	INTEGER
sslcertid	optional	Gives back only the record that contains the specified sslcertid.	TEXT
mincreateddate	optional	Limit your search to objects that have been created after mincreateddate	TEXT
maxcreateddate	optional	Limit your search to objects that have been created before maxcreateddate	TEXT
minupdateddate	optional	Limit your search to objects that have been last modified after minupdateddate	TEXT
maxupdateddate	optional	Limit your search to objects that have been last modified before maxupdateddate	TEXT
minexpirationdate	optional	Limit your search to objects that will expire after minexpirationdate	TEXT
maxexpirationdate	optional	Limit your search to objects that will expire before maxexpirationdate	TEXT

Returned Properties and Values

Code	Description
200	Command completed successfully
541	The command failed

Property	Description
sslcertid[n]	The unique object ID numbers (16 hex digits) in the system
Total	Total count of records
First	Index of the first element in the response
Count	How many records are given back in that query
Last	Index of the last element in the response
Limit	As chosen in the request
sslcertcn[n]	Common Name (= domainname) for which the cert has been signed. Only available with parameter wide set to 1.
sslcertstatus[n]	Status information: Either ACTIVE or PENDING. Only available with parameter wide set to 1.
sslcertcreateddate[n]	Dates of creation. Only available with parameter wide set to 1.
sslcertupdateddate[n]	Dates of last update. Only available with parameter wide set to 1.
Sslcertexpirationdate[n]	Dates of expirations. Only available with parameter wide set to 1.
User[n]	Subuser, that is the cert owner. Only available with parameter wide set to 1.
Parentuser[n]	Direct parentusers of the cert owner users. Only available with parameter wide set to 1.
Sslcertclass[n]	Product classes (like THAWTE_SSL123) of the certs. Only available with parameter wide set to 1.

Notes:

- none

4.1.4 ParseSSLCertCSR

Description

Parses the information that is contained in a CSR (certificate sign request) and gives back common name (=domainname), company informations like email-address and so on. The command can be used to check the validity of a CSR-File.

Availability

No limitations

Input Parameters

submit the request using the following syntax:

```
BASE-URL?s_login=reseller.de&s_pw=secret&command=command&parameter1=value1&parameter2=value2&parameter3=value3...
```

Parameter	Obligation	Definition	Type
s_login	required	Login ID of the user account	TEXT
s_pw	required	Account password	TEXT
s_user	optional	User ID of the user as which the command shall be executed (must be a subuser of s_login)	TEXT
command	required	Name of command to be executed, here: command=ParseSSLCertCSR	TEXT
csr0...csrN	required	The certificate sign request (CSR) by line, represented as csr0, csr1, csr2, ... , csrN: csr0 = -----BEGIN CERTIFICATE REQUEST----- csr1 = A34)\$/45BF... csr2 = 1E.. csr3 = ... csrN = ----- END CERTIFICATE REQUEST -----	TEXT

Returned Properties and Values

Code	Description
200	Command completed successfully
541	The command failed

Property	Description
CN	Common Name (= domainname)
O	Owner Name or Company
ST	State
C	2 letter County Code (i.e. "DE")
EMAILADDRESS	Mailaddress that has been compiled into the CSR
L	City

Notes:

- none